UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/633,907	08/04/2003	Peter Szor	SYMC1035	7555

34350 7590 05/23/2006

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER	
ALPHONSE, FRITZ	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 05/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/633,907	SZOR, PETER	
	Examiner	Art Unit	
	Fritz Alphonse	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,6,8-17 and 19* is/are rejected.

7)☒ Claim(s) *2,5,7,18 and 20* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

0.1 This office action is in response to amendment filed on 2/21/2006. Claims 1, 12 and 17 are amended. Claims 1-20 are pending.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3-4, 6, 8-17, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khazan (US Pub. No. 20050108562 A1) in view of Szor (US Pub. 2004/0158725 A1).

As to claim 12, Khazan discloses (fig. 4A; [0040]) shows a malicious code detection device (110) including: an intercept module (114; [0073]) for intercepting a request issuing on a host computer system prior to the sending of the request from the host computer system to a target computer system; an analyzer module (108; [0076]) coupled to the intercept module (114); Khazan discloses a request database (see figs. 1, 4A) coupled to the analyzer module, the request database including one or more request entries, each of the one or more request entries identifying a request determined to be suspicious (114; [0032]); and a standards list (106) coupled to the analyzer module (108; see [0040; [0072; 0078]).

Khazan differs from claims 12 in that he does not specifically teach a standard list including selected standards for use in determining whether the request is suspicious. However, referring to fig. 3, Szor shows a system including selected standards for use in determining whether a request is suspicious (see [0025]).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to combine Khazan with the dynamic detection of computer worms, as disclosed by Szor. Doing so would provide a truly dynamic malicious code detection system, which is capable of filtering outgoing traffic on the packet level as well as on the stream level.

As to claims 13-14, Khazan discloses a malicious code detection device comprising an inclusion profile list (112) coupled to the analyzer module (104-108).

As to claims 15-16, Khazan discloses a malicious code detection device, further comprising a memory (data storage system 12) area coupled to the intercept module (114) and the analyzer module (see [0072]); and, wherein the intercept module (114) includes an interception mechanism for intercepting a request ([0073]).

As to claims 1 and 3, method claims 1 and 3 correspond to apparatus claim 12; therefore, they are analyzed as previously discussed in claim 12 above.

As to claims 17 and 19, the claims have substantially the limitations of claim 12; therefore, they are analyzed as discussed in claim 12 above.

As to claims 4, 6 and 8, Khazan discloses a method, further releasing the request upon a determination that the request is not suspicious (fig. 8; [0094]).

As to claim 9-11, Khazan discloses a method, wherein the request is an HTTP GET request; and, wherein the intercepting a request on a host computer system occurs at the application level ([0036; 0045]).

Allowable Subject Matter

3. Claims 2, 5, 7, 18 and 20 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

4. Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection. The prior art of Szor has been added for new ground of rejection.

Conclusion

5. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231

or faxed to: (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fritz Alphonse, whose telephone number is (571) 272-3813. The examiner can normally be reached on M-F, 8:30-6:00, Alt. Mondays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert De Cady, can be reached at (571) 272-3819.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-3824.

Information regarding the status of an application may also be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fritz Alphonse

Art Unit 2133

May 10, 2006

GUY LAMARRE
PRIMARY EXAMINER